



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/360,068 | 07/23/1999 | KEVIN J. PAGE | 2322-0482 | 3638 |

27111 7590 03/15/2004

BROWN, MARTIN, HALLER & MCCLAIN LLP
1660 UNION STREET
SAN DIEGO, CA 92101-2926

EXAMINER

KLIMACH, PAULA W

ART UNIT PAPER NUMBER

2135

DATE MAILED: 03/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/360,068

Applicant(s)

PAGE ET AL.

Examiner

Paula W Klimach

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 December 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-58 is/are pending in the application.
- 4a) Of the above claim(s) 36-58 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-35 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 4, 5, 9, and 11.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Applicant elected group II, claims 1-35 without traverse in Paper No. 14, dated 1/15/04. Thus, claims 36-58 are drawn to non-elected invention and withdrawn from further consideration.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. **Claims 1, 2, 18, 29, 30** are rejected under 35 U.S.C. 102(e) as being anticipated by Hohle et al (6,101,477).

In reference to claims 1 and 29, Hohle teaches a system for establishing a secure connection between a smart card and a central computer (issuer 10), Fig.10. The system uses the method of modulating an outgoing secure radio frequency signal transmitted from the smart card to produce an out going secure data signal, column 3 lines 31-51. The connection described by Hohle is a secure connection because the system uses the DES algorithm for encryption of a random number in the challenge/response authentication, column 11 line 63 to column 12 line 36. Since that data is sent over the network disclosed in Fig. 10, it must be formatted in accordance with a communication network protocol to produce an outgoing format. Finally, in column 5 line 64 to column 6 line 4, the formatted signal is sent to the central computer system,

Art Unit: 2135

issuer 10. The card is described as communicating with the issuer 10 through the client host (the access point) and therefore the for communication to take place a signal must be sent from the card to the central computer system.

In reference to claims 2 and 30, Hohle subjects the out going data to a security function only in the smart card and the central computer system. The data is "signed" by the central computer by producing the MAC, column 22 lines 53-58. The card then produces a MAC based on the received message and compares them and the two MACs will not match if the message or the wrong key has been used, column 22 lines 59-67.

In reference to claim 18, Hohle discloses a system where data is exchanged with a smart card through radio frequency communication, column 3 lines 31-51. The data is exchanged with a central computer, the issuer 10, through a network, Fig. 10. The security function performed on the data is as discussed in reference to claim 2.

In reference to claim 19, the security function is as discussed in the reference to claim 2.

In reference to claim 20, since the data is transported over the network as shown in Fig 10, the data is evidently formatted in accordance with the communication network protocol for the network in Fig. 10, and reformatted at the central computer. The data is transmitted through the communication network as shown in Fig. 10.

Claim Rejections - 35 USC § 103

4. **Claims 3-17 and 31-34** are rejected under 35 U.S.C. 103(a) as being unpatentable over Hohle as applied to claim 1 and 29 above, and further in view of Wilson (5,295,188).

In reference to claims 3, 31, and 32, Hohle discloses a proximity (contact free) card system in communication with a central computer. However, Hohle does not disclose a system where the outgoing secure signal is not deciphered after demodulation.

Wilson discloses a system for public key encryption and decryption where data is encrypted by a smart card and decrypted at the central location, column 16 lines 25-47.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the signal in the smart card as in Wilson and then to transport the signal as disclosed by Hohle. One of ordinary skill in the art would have been motivated to do this because smart cards are inexpensive authentication devices, Wilson column 2 lines 5 and 6.

In reference to claim 4, the data at the central computer (the bank computer 150) is transformed back into plain text, column 16 lines 45-47. The data is sent over the network to the central computer, column 16 line 34, as a result, it is apparent that it must have been reformatted.

In reference to claim 5, the system disclosed by Hohle receives the incoming secure formatted signal from the central computer as discussed in claim 1. Wilson teaches that communication in the opposite direction, in this case from the central computer to the smart card, may be performed in the same way, column 15 lines 30-43.

In reference to claims 6 and 33, the Hohle reference teaches of contactless cards using phase, frequency and amplitude modulation, column 3 lines 44-45, therefore the reader demodulates the signal sent over radio frequencies. Wilson teaches applying cipher text to a decryption module to arrive at the plain text, column 15 lines 30-51.

In reference to claim 7, the security function is as discussed above in the discussion for claim 6.

In reference to claims 8 and 34, the data is encoded in the smart card, as discussed for claim 3, which would make the outgoing data signal secure.

In reference to claim 9, Hohle further teaches generating a MAC at the smart card and then appending it to the outgoing data as a electronic seal to sign the data, column 22 lines 47-67.

In reference to claim 10, 11, 15, 16, and 35, Hohle discusses the use of a MAC to seal messages with in order to detect an unauthorized modification of the outgoing data, column 22 lines 47-67.

In reference to claim 12, Wilson discusses the use of a smart card to encrypt data using software stored on the card, column 16 lines 25-32. Wilson further discloses being able to perform the communication in the opposite direction, column 15 lines 41-43.

In reference to claim 13, encoding data from the smart card was discussed in reference to claim 3. Wilson further discusses performing the communication in the opposite direction, column 15 lines 41-43, from the central computer to the smart card (from B to A).

In reference to claim 14, Hohle discloses a system where a MAC and appended to the message, column 22 lines 47-67.

In reference to claim 17, encoding using a smart card and transmitting the radio frequencies are discussed in reference to claim 3. The modulation of the outgoing radio frequency, formatting of the secure data, and the transmission of outgoing data has been discussed in reference to claim 1. The reformatting of the outgoing secure signal and decoding of the signal has been discussed in reference to claim 4. While the reference to claim 8 discusses the encoding of information from the central computer. It is evident that since the signal is sent over the network, it would be formatted to produce an incoming formatted signal. The reference

Art Unit: 2135

to claim 5 discusses the receiving, reformatting, and transmission of the secure signal. Finally the demodulation and the decoding of the secure data signal is discussed in reference to claim 6.

5. **Claims 21-25** are rejected under 35 U.S.C. 103(a) as being unpatentable over Hohle in view of Murphy et al (6, 226, 744 B1).

In reference to claim 21, Hohle discloses a system for communication between a smart card and a central computer with the ability for some of the software to exist outside the card and be downloaded during transaction, column 4 lines 49-54. The secure data is exchanged with the smart card reader using radio frequency communication, column 3 lines 42-45. However Hohle does not disclose a system where interface software can be downloaded.

Murphy discloses a system where a user can download a smart card interface module to the client terminal, column 6 lines 8-25.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the Client terminal 14 described by Murphy to the network described by Hohle and using the smart card and smart card reader disclosed by Hohle. One of ordinary skill in the art would have been motivated to do this because users would be able to access restricted information with the smart card without having to install software, column 3 lines 24-28.

In reference to claim 22, the secure data is exchanged over a baseband channel, Murphy fig 1 where the smart card reader is connected to a client terminal, which then connects to the network. Hohle discloses a system that exchanges data with a central computer.

In reference to claims 23 and 24, Hohle further describes a system where the central computer creates the MAC and the smart card calculates it and compares it to the MAC that it expects and it is not calculated during transmission, column 22 lines 47-67.

In reference to claim 25, the smart card reader described by Murphy is connected to a client terminal, Fig. 1. The smart card reader described by Hohle is a proximity card, Hohle column 3 lines 31-50. In Hohle Fig. 10 the access points are connected to a network. The central computer calculates the MAC and therefore has a security device coupled to it, column 22 lines 47-67

In reference to claim 26, the client terminal in Murphy works on the Internet, Fig. 1.

In reference to claim 27 and 28, claim 27 is the same discussion as in the reference to claim 23 and 24.

Art Unit: 2135

Conclusion

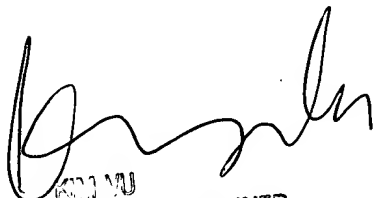
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Fri 7:15 a.m to 3:45 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes can be reached on (703) 305-9711. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-8421 for regular communications and (703) 305-8421 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-4832.

PWK

Friday, March 05, 2004


PAULA W. KLIMACH
PATENT EXAMINER
TECHNOLOGY CENTER 2100